On the second weight of generalized Reed-Muller codes

O. Geil

Aalborg University

ACA - July 2008

Error correcting codes - Linear codes

Purpose: Reliable communication over noisy channels.

Definition:
A linear code C is a k-dimensional subspace of $\mathbf{F}_q^n$.

Choose an isomorphism from $\mathbf{F}_q^k$ to C.

Encode message $\vec{m} = (m_1, \ldots, m_k) \in \mathbf{F}_q^k$ to its image $\vec{c} = (c_1, \ldots, c_n) \in C$ (called a codeword).

Error correction

$\vec{c}$ is send over channel, but noise $\vec{e}$ is added.

Receiver gets: $\vec{r} = \vec{c} + \vec{e}$.

Idea:
If only few e_i's are non-zero and if codewords in C are "far" from each other, then receiver can recover $\vec{c}$ by choosing codeword "nearest" to $\vec{r}$.

Weights and distances

$\vec{a}, \vec{b} \in \mathbf{F}_q^n$.

$w_H(\vec{a}) = \#\{i \mid a_i \neq 0\}$.

$\text{dist}_H(\vec{a}, \vec{b}) = \#\{i \mid a_i \neq b_i\} = w_H(\vec{a} - \vec{b})$.

$$\begin{aligned} d &= \min\{w_H(\vec{c}) \mid \vec{c} \in C \backslash \{\vec{0}\}\} \\ &= \min\{dist_H(\vec{a}, \vec{b}) \mid \vec{a}, \vec{b} \in C, \vec{a} \neq \vec{b}\} \end{aligned}$$

is called minimum distance (or minimum weight).

If $w_H(\vec{e}) \leq \lfloor \frac{d-1}{2} \rfloor$ then nearest codeword to $\vec{r} = \vec{c} + \vec{e}$ is $\vec{c}$.

Decoding strategies

- Minimum distance decoding. Radius is $\lfloor (d-1)/2 \rfloor$.
- List decoding. Radius is larger than $\lfloor (d-1)/2 \rfloor$.
- Maximum likelihood decoding. Look for nearest codeword.

Weight distribution is $\{W_1, \ldots, W_n\}$ where
$W_i = \#\{\vec{c} \in C \mid w_H(\vec{c}) = i\}$.

Weight distribution = Distance distribution.

Weight distribution tells you how good is List decoding and Maximum likelihood decoding.

Generalized Reed-Muller codes

$$\mathbf{F}_q^m = \{P_1, \ldots, P_{q^m}\}.$$

$$\begin{aligned} \mathrm{RM}_q(s,m) \quad = \quad & \{(F(P_1), \ldots, F(P_{q^m})) \mid F \in \mathbf{F}_q[X_1, \ldots, X_m], \\ & \deg(F) \leq s, \deg_{X_i}(F) < q, \quad \text{for } \; i = 1, \ldots, m\} \end{aligned}$$

Question 1a:
How many zeros can a multivariate q-ary polynomial of total degree s possibly have?

Question 1b:
What is the minimum distance of $\mathrm{RM}_q(s, m)$?

Question 2a:
What is the second highest number of attainable zeros for a multivariate q-ary polynomial of total degree s?

Question 2b:
What is the second weight of $\mathrm{RM}_q(s, m)$?

Parameters for $\mathrm{RM}_q(s, m)$

- Minimum distance. Kasami, Lin, Peterson 1968. The BCH-bound.
- Various results on weight distribution for $q = 2$.
- For $s \leq 2$ weight distribution. McEliece 1969.
- Second weight for small dimensions. Cherdieu, Rolland 1996. Geometric arguments.
- Second weight for $s < q/2$. Sboui 2007. Geometric arguments.
- Some results on third weight. Rodier, Sboui in 2008. Geometric arguments.
- Second weight for $s < q$ (and for high values of s). O.G. in 2008. Ideal-variety approach.
- Second weight for all s (except $s \equiv 1 \mod (q-1)$). Rolland, recent preprint. Ideal-variety approach.

The ideal-variety approach

Find (or estimate)

$$\begin{aligned} & \#\mathbf{V}_{\mathbf{F}_q}(\langle F(X_1,\ldots,X_m)\rangle) \\ = \; & \#\mathbf{V}_{\mathbf{F}_q}(\langle F(X_1,\ldots,X_m), X_1^q - X_1,\ldots,X_m^q - X_m\rangle) \\ = \; & \#\mathbf{V}_{\bar{\mathbf{F}}_q}(\langle F(X_1,\ldots,X_m), X_1^q - X_1,\ldots,X_m^q - X_m\rangle). \end{aligned}$$

General set-up

Problem: Given $I \subseteq \mathbf{F}_q[X_1, \ldots, X_m]$ find $\#\mathbf{V}_{\mathbf{F}_q}(I)$.

Solution:

$$\Delta_{\prec}(J) = \{X_1^{i_1} \cdots X_m^{i_m} \mid X_1^{i_1} \cdots X_m^{i_m} \text{ is not leading monomial of any polynomial in } J\}$$

$$I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle.$$

$$\#\mathbf{V}_{\mathbf{F}_q}(I) = \#\Delta_{\prec}(I_q).$$

An easy proof of $\#\mathbf{V}_{\mathbf{F}_q}(I_q) \leq \#\Delta_{\prec}(I_q)$

Given Gröbner basis $\mathcal{G}$ then division with remainder mod $\mathcal{G}$ is unique. Hence,

$$\{M + J \mid M \in \Delta_{\prec}(J)\}$$

is a basis for $\mathbf{F}_q[X_1, \ldots, X_m]/J$.

Let $\mathbf{V}_{\mathbf{F}_q}(I_q) = \{P_1, \ldots, P_n\}$. The map

$$\mathrm{ev} : \mathbf{F}_q[X_1, \ldots, X_m]/I_q \to \mathbf{F}_q^n$$

$$\mathrm{ev}(F + I_q) = (F(P_1), \ldots, F(P_n))$$

is a surjective homomorphism.

QED

To see surjective...

Write $P_j = (P_j^{(1)}, \ldots, P_j^{(m)})$. Then

$$\mathrm{ev}\Big(\big(\prod_{s=1,\ldots,m} \prod_{\substack{j=1,\ldots,n \\ P_j^{(s)} \neq P_i^{(s)}}} (X_s - P_j^{(s)})\big) + I_q\Big)$$

is nonzero in position i, but zero elsewhere.

Proof of $\#\mathbf{V}_{\mathbf{F}_q}(I_q) = \#\Delta_{\prec}(I_q)$

Proof of injectivity involves

- radical ideals
- algebraic closure
- strong Nullstellensatz.

Monomial ordering

Mostly for simplicity, assume $\prec$ is degree lexicographic ordering.

$X_1^{a_1} \cdots X_m^{a_m} \prec X_1^{b_1} \cdots X_m^{b_m}$ if either 1. or 2.

1. $a_1 + \cdots + a_m < b_1 + \cdots + b_m$
2. $a_1 + \cdots + a_m = b_1 + \cdots + b_m$ but $X_1^{a_1} \cdots X_m^{a_m} \prec_{lex} X_1^{b_1} \cdots X_m^{b_m}$

Minimum distance of $\mathrm{RM}_q(s,m)$

$$F(X_1,\ldots,X_m) \in \mathbf{F}_q[X_1,\ldots,X_m]$$

$$\deg_{X_i}(F) < q,\ i = 1,\ldots,m.$$

$$\mathrm{lm}(F) = X_1^{i_1}\cdots X_m^{i_m},\ \ i_1+\cdots+i_m \le s.$$

$$\begin{aligned} & \#\Delta(\langle F(X_1,\ldots,X_m), X_1^q - X_1,\ldots,X_m^q - X_m\rangle) \\ \le\ & \#\Delta(\langle X_1^{i_1}\cdots X_m^{i_m}, X_1^q,\ldots,X_m^q\rangle) \\ =\ & q^m - \prod_{l=1}^{m}(q-i_l) \end{aligned}$$

Minimum distance - cont

Let $s = a(q-1)+b$, $0 \leq b < q-1$.

$i_1 + \cdots + i_m \leq s$, $i_1 < q, \ldots, i_m < q$

$\max\{q^m - \prod_{l=1}^{m}(q-i_l)\} = q^m - (q-b)q^{m-a-1}$.

On the other hand, polynomial
$(X_1^{q-1}-1)\cdots(X_a^{q-1}-1)(X_{a+1}-\alpha_1)\cdots(X_{a+1}-\alpha_b)$
has this amount of zeros.

Second weight for $s < q$

Proposition:
If $F(X_1, \ldots, X_m)$ is of total degree s then either sq^{m-1} zeros or at most $sq^{m-1} - (s-1)q^{m-2}$ zeros. Both values can be realized.

$\mathrm{Im}(F) = X_1^{i_1} \cdots x_m^{i_m}$

Case 1: $i_1 < s, \ldots, i_m < s$

$$\begin{aligned} & \#\Delta(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, \ldots, X_m^q \rangle) \\ = \quad & q^m - \prod_{l=1}^{m} (q - i_l) \end{aligned}$$

is at most $sq^{m-1} - (s-1)q^{m-2}$

Second weight for $s < q$, cont.

Case 2: $i_1 = s, i_2 = \cdots = i_m = 0$

$$\begin{aligned} H(X_1, \ldots, X_m) &= S(X_1^q - X_1, F(X_1, \ldots, X_m)) \\ &= X_1^q - X_1 - X_1^{q-s} F(X_1, \ldots, X_m) \end{aligned}$$

Total degree of H at most q.

$R(X_1, \ldots, X_m) =$
$H(X_1, \ldots, X_m)$ rem $(F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m)$.

If $R(X_1, \ldots, X_m) = 0$ then $\{F, X_1^q - X_1, \ldots, X_m^q - X_m\}$ a GB and sq^{m-1} zeros.

case 2 - cont

$\mathrm{lm}(R) = X_1^{v_1} \cdots X_m^{v_m}$.
$\sum_{i=1}^{m} v_i \leq q, v_1 < s, v_2 < q, \ldots, v_m < q$.

$$
\begin{aligned}
& \#\Delta(\langle F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m \rangle) \\
\leq\ & \#\Delta(\langle X_1^s, X_2^q, \ldots, X_m^q, X_1^{v_1} \cdots X_m^{v_m} \rangle) \\
=\ & sq^{m-1} - (s - v_1) \prod_{i=2}^{m} (q - v_i) \\
\leq\ & sq^{m-1} - (s-1)q^{m-2}
\end{aligned}
$$

There are simple polynomials with exactly $sq^{m-1} - (s-1)q^{m-2}$ zeros.

$(m-1)(q-1) < s$

$d(\mathrm{RM}_q(s-1,m)) = d(\mathrm{RM}_q(s,m)) + 1$

Hence, second weight is $d+1$

Second weight for $\mathrm{RM}_q(s,2)$ covered.

...very recently

... Robert Rolland used method from this talk plus a technical lemma to find remaining second weights

...except for the case $s = a(q-1)+1$...